

ABSTRACT

**AN AUTHENTICATION PROTOCOL FOR ESTABLISHING A
MOMENTARY TRUST ZONE DURING A LOGIN AND OPERATION
PROCEDURE**

5

The present invention discloses an authentication protocol for establishing a momentary trust zone during a login and operation procedure. The protocol involves a user interface (20) which interacts with a user, a personal cryptographic key generator
10 (10) which can be activated by the user to generate ephemeral keys and/or sign credentials, a cryptographic processor (30) which is embedded within the user interface to challenge and verify the authenticity of the user interface (20), and a verification processor (40) which is embedded within service provider servers to verify processed data received from the cryptographic processor (30). The personal
15 cryptographic key generator (10) can be further characterised by (a) operating entirely in an offline mode with the exception of a single instance where it (10) is switched to an online mode to transmit the generated ephemeral keys and/or the signed credentials, and after which it switches back to the offline mode, and (b) operating in an unbalance communication mode where the personal cryptographic key generator
20 (10) exclusively initiates and/or disconnects a data transfer link to a device which the user interface (20) is operated thereon.

(Fig. 1)